Item 4b-Attachment 2A

AGENDA ITEM 4b
ACCEPTANCE OF RISK SUMMARY
AS OF DECEMBER 31, 2010

Audit (Report Issue Date): Review of Information Security (08/19/02)

Division responsible: Information Security Office

Finding 4.6 Description:
Hiring procedures do not require background checks for information security staff and other sensitive positions.

Current Status:
COMPLETE. The Information Security Office is accepting the risk of not performing background checks at this time. There are no regulatory requirements that background checks be performed. This issue will be tracked by the CalPERS' Enterprise Risk Management for future consideration.

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

Division responsible: Information Security Office

Finding 1.2 Description:
CalPERS implements security measures to protect information assets housed at CalPERS. Information Security Office should implement required specifications and assess whether each addressable specification is a reasonable safeguard in the environment.

Current Status:
COMPLETE. The Information Security Office is accepting the risk of possible non-compliance with this HIPAA Security requirement. The Information Security Office has provided various documents to demonstrate that all systems that contain ePHI have been identified, and that a risk assessment of potential risks and vulnerabilities has been performed. However, the Information Security Office has not provided documentation demonstrating that various roles and responsibilities with regard to implementing and monitoring selected controls have been clearly defined and communicated, as well as that appropriate security measures are sufficient to reduce identified risks have been implemented. With the pending implementation of PSR, it is not feasible to implement additional controls beyond those currently implemented. The Information Security Office will conduct a risk assessment within six months of PSR deployment to assess compliance with HIPAA requirements.

Finding 1.4 Description:
CalPERS' Event Logs Practice requires specific security events be logged at key servers. However, the practice does not specify which events must be logged at the system, application, and user level. Information Security Office should develop an Information System Activities Review Practice.

Current Status:
COMPLETE. The Information Security Office is accepting the risk for not taking steps to ensure that CalPERS' current Security Practices appropriately address the types of information system activities that should be recorded and reviewed at all levels, the frequency that the reviews should occur, as well as clearly defining the parties

AGENDA ITEM 4b
ACCEPTANCE OF RISK SUMMARY
AS OF DECEMBER 31, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

responsible for recording and monitoring the various types of activities. With the pending implementation of PSR, it is not feasible to retrofit legacy systems. The Information Security Office will conduct a risk assessment within six months of PSR deployment to assess compliance with HIPAA requirements and addressable specifications, including logging requirements and whether threats and vulnerabilities are being managed.

Finding 15.1 Description:
CalPERS' Event Logs Practice does not require a retention period of 6 years or recording of functions performed. Information Security Office should modify the Event Logs Practice to require the recording and retention requirements.

Current Status:
COMPLETE. The Information Security Office is accepting the risk for not taking steps to ensure that CalPERS' current Security Practices appropriately identify the functions that need to be recorded, as well as the retention period for said information to ensure compliance with the applicable section of the HIPAA law. With the pending implementation of PSR, it is not feasible to retrofit legacy systems. The Information Security Office will conduct a risk assessment within six months of PSR deployment to assess compliance with HIPAA requirements and addressable specifications, including logging requirements and whether threats and vulnerabilities are being managed.

Finding 15.2 Description:
The Document Management System does not log who viewed imaged documents, when and where the imaged documents are created, printed, exported, or viewed. The Event Logs Practice should be modified to provide clearer guidelines.

Current Status:
COMPLETE. The Information Security Office is accepting the risk for not taking steps to ensure that CalPERS' current Security Practices provides an appropriate level of guidance regarding events and attributes that should be logged, maintained, and periodically reviewed, to ensure compliance with the applicable sections of the HIPAA law. With the pending implementation of PSR, it is not feasible to retrofit legacy systems. The Information Security Office will conduct a risk assessment within six months of PSR deployment to assess compliance with HIPAA requirements and addressable specifications, including logging requirements and whether threats and vulnerabilities are being managed.

AGENDA ITEM 4b
ACCEPTANCE OF RISK SUMMARY
AS OF DECEMBER 31, 2010

Audit (Report Issue Date):	**Review of Internal Controls - FISMA (12/17/07)**
Division responsible:	Information Technology Services Branch

Finding 1.5 Description:
Password configuration enforcement was reviewed for ACES, COMET, CRS, PA Billing, RIBS, and SCBA systems. It was noted that the systems’ configurations do not always comply with the requirements specified in the security practice. The degree and area of noncompliance varies by system.

Current Status:
COMPLETE. The Information Technology Services Branch is accepting the risk associated with this finding regarding various systems' password configuration compliance with CalPERS' security practice. There has been minimal risk associated with password configuration variances in the legacy systems reviewed to justify the additional man hours and cost to address the issue. PSR will replace these systems and password configuration will be addressed when PSR is deployed in September 2011.